

AMENDMENTS TO THE SPECIFICATION:

Please replace the paragraph beginning on page 1, line 10 with the following amended paragraph:

In recent years, communication ~~terminals~~ ~~terminals~~, such as personal computers (PCs) with a communication performance, have frequently been involved in information-service network communication systems that require each communication terminal to be authenticated. In such a typical system, a communication terminal is used, which is entitled to operate SSL (Security Sockets Layer) with a technique of encrypting documents to be transferred in forms. A server system incorporated in such a system receives user-identifying information, such as a password, given from such communication terminal through communication means such as the Internet, and authenticates the communication terminal (i.e., a user who handles such communication terminal). Thus, only when it is determined that the authentication reveals an affirmative result, the server system is permitted to provide the communication terminal with data requested by the user (i.e., data service).

Please replace the paragraph beginning on page 2, line 7 with the following amended paragraph:

In order to accomplish the above object, as one aspect of the present invention, there is provided an authentication system in which a communication terminal is communicably connected to a server system via communication means, wherein an authenticated result for a user who handles the communication ~~communication~~ terminal is made reference to provide data from the server system to the communication terminal via the communication means, the server system comprising: a first authentication unit configured to authenticate user-identifying information transmitted from the communication terminal and generate first key information based on the user-identifying information so that the first key information is transmitted from the server system to the communication terminal; a second authentication unit configured to authenticate the first key information transmitted from the communication terminal and generate second key information to access the data based on the first key information so that the second key information is transmitted from the server system to the communication terminal; and an

access permitting unit configured to permit the data to be accessed within a predetermined period of time, the access being carried out on the basis of the second key information transmitted from the communication terminal.

Please replace the paragraph beginning on page 3, line 13 with the following amended paragraph:

As another aspect of the present invention, there is provided a server system communicably connected with a communication terminal via communication means, wherein an authenticated result for a user who handles the communication ~~communicarian~~ terminal is made reference to provide data from the server system to the communication terminal via the communication means, the server system comprising: a first authentication unit configured to authenticate user-identifying information transmitted from the communication terminal and generate first key information based on the user-identifying information so that the first key information is transmitted from the server system to the communication terminal; a second authentication unit configured to authenticate the first key information transmitted from the communication terminal and generate second key information to access the data based on the first key information so that the second key information is transmitted from the server system to the communication terminal; and an access permitting unit configured to permit the data to be accessed within a predetermined period of time, the access being carried out on the basis of the second key information transmitted from the communication terminal. Hence, this server system has the advantages identical to those described ~~descried~~ in the foregoing authentication system.

Please replace the paragraph beginning on page 3, line 34 with the following amended paragraph:

It is preferred that the first key information is an access key to access to the data stored in the server system and the second key is a session ~~ession~~ key for transmission control of the data. Therefore, under the authentication with no SSL employed, the first and second key information can be used as a kind of password, thus eliminating the necessity of adopting the password.

Please replace the paragraph beginning on page 4, line 19 with the following amended paragraph:

As ~~another~~ another aspect of the present invention, there is provided an authentication method, in which a communication terminal is communicably connected to a server system via communication means, wherein an authenticated result for a user who handles the communication ~~communication~~ terminal is made reference to provide data from the server system to the communication terminal via the communication means, comprising the steps of: authenticating user-identifying information transmitted from the communication terminal; generating first key information based on the user-identifying information so that the first key information is transmitted from the server system to the communication terminal; authenticating the first key information transmitted from the communication terminal; generating second key information to access the data based on the first key information so that the second key information is transmitted from the server system to the communication terminal; and permitting the data to be accessed within a predetermined period of time, the access being carried out on the basis of the second key information transmitted from the communication terminal. Hence, this method is able to provide the advantages identical to those described ~~described~~ in the foregoing authentication system.

Please replace the paragraph beginning on page 5, line 2 with the following amended paragraph:

By way of example, the first key information is an access key to access to the data stored in the server system and the second key is a session ~~session~~ key for transmission control of the data. When using this technique, there is no necessity of adopting a password.

Please replace the paragraph beginning on page 5, line 6 with the following amended paragraph:

Still, as another aspect of the present invention, there is provided a computer-readable program installed in a server system communicably connected with a communication terminal via communication means, wherein an authenticated result for a user who handles the communication ~~communication~~ terminal is made reference to provide data from the server

system to the communication terminal via the communication means, the program makes a computer realize the functions of: first authentication means for authenticating user-identifying information transmitted from the communication terminal and generate first key information based on the user-identifying information so that the first key information is transmitted from the server system to the communication terminal; second authentication means for authenticating the first key information transmitted from the communication terminal and generate second key information to access the data based on the first key information so that the second key information is transmitted from the server system to the communication terminal; and access permitting means for permitting the data to be accessed within a predetermined period of time, the access being carried out on the basis of the second key information transmitted from the communication terminal. Hence, this program makes it possible to provide the server system with the advantages identical to those described ~~described~~ in the foregoing authentication system.

Please replace the paragraph beginning on page 6, line 19 with the following amended paragraph:

Fig. 9 details the processing at step S3 in Fig. 6, which is the processing for easy sign-up ~~sign-up~~;

Please replace the paragraph beginning on page 8, line 15 with the following amended paragraph:

Meanwhile, the server system 1 has the configuration that enables communication of various types of key information with the PC 3 (or mobile phone 4), which is carried out as follows. That is, when receiving, from the navigation terminal 5 via the Internet IN, the user accounts that were given through the PC 3 (or mobile phone 4), the server system 1 performs authentication on the user accounts, so that, if the authentication succeeds, the server system 1 provides the navigation terminal 5 with an access key serving as the first key information. When receiving the access key and the user ID from the navigation terminal 5 via the Internet IN, the server system 1 authenticates the received ~~receive~~ access key, so that, if the authentication succeeds, the server system 1 provides the navigation terminal 5 with a session key serving as the second key information. Moreover, in the case of receiving the session key from the

navigation terminal 5 through the Internet IN, the server system 1 gives the navigation terminal 5 data that are desired by the user.

Please replace the paragraph beginning at page 9, line 28 with the following amended paragraph:

The database unit 15 memorizes all kinds of data necessary for navigation processing, such data including, as shown in Figs. 2 and 3, user's name, address, telephone number, mail address, application number, credit card number, expiration date of credit card, user ID (identification), password, license number, access key, manufacture ID, model number ID, hardware number, session key, and expiration time of session key; map data to be displayed on a display screen of the navigation terminal 5, various kinds of data required for route processing, both positional data and content data at various points on a map to be displayed on the display screen of the navigation terminal 5; point data necessary for execution of navigation processing; and users' data about users who use the navigation terminal 5. These kinds of data are read out at necessary timing from the database 15 and sent to the system controller 13 ~~controller 13~~.

Please replace the paragraph beginning on page 11, line 17 with the following amended paragraph:

Then, the user is to input a credit card number and other necessary data on the portal site, so that those pieces of information are sent to the server system 1 on the SSL ~~SSL~~ for user registration. The server system 1 responds to this transmission by issuing user accounts (i.e., user ID, password, and license number) and sending these user accounts on the SSL to the user's PC 3 (step S2).

Please replace the paragraph beginning on page 12, line 13 with the following amended paragraph:

The server system 1 provides the navigation terminal 5 with the designated data, such as map data, via the Internet ~~Internet~~ IN until a period of valid time (for example, 5 minutes) given to the session key will expire (NO at step S5). When the valid period of time of the

session key expires (YES at step S5), the processing in Fig. 1 is ~~returned~~ retuned to step S4, thereby permitting the user to acquire the session key again as long as the user desires.

Please replace the paragraph beginning on page 13, line 12 with the following amended paragraph:

Hence the user inputs an application number into the ~~PC 3~~ PC3 to transmit data indicative of the application number toward the server system 1 on the SSL (steps S25 and S26). In response to this, the server system 1 accepts the data of the application number to make the application number undergo authentication carried out therein. On completion of the authentication of the application number (provided that the authentication succeeds), the server system 1 sends back information indicative of a payment screen to the user's PC 3 on the SSL, thus the payment screen being displayed on the PC 3 (steps S27 to S29).

Please replace the paragraph beginning on page 17, line 1 with the following amended paragraph:

At step S77, the server system 1 transmits to the navigation terminal 5 the session key with the valid time or the error code. When receiving the notification of the arrival of such information at step S78, in the navigation terminal 5, it is determined whether or not the session ~~ession~~ key has been received (step S79). If the session key has been received (YES at step S79), the session key and its valid time as well as the user ID, access key and license number are stored in the memory unit 20 of the navigation terminal 5 (step S80), and then the processing is terminated. Further, when the session key has not been received (NO at step S79), the processing is also brought to an end.

Please replace the paragraph beginning on page 18, line 35 with the following amended paragraph:

As described above, the authentication system for communication apparatuses according to the present embodiment is equipped with the server system 1, in which the common authentication unit 12 and system controller 13 are placed. The common authentication unit 12 authenticates user accounts sent from the PC 3, generates an access key based on the user

accounts, and allows the generated access key to be transmitted from the server system 1 to the navigation terminal 5. The common authentication unit 12 also authenticates the access key sent from the navigation terminal 5, generates a session key to access data to be serviced, such as map data, on the basis of the access key, and allows the generated session key to be transmitted from the server system 1 to the navigation terminal 5. The system controller 13 permits an access of the navigation terminal 5 to the server system 1 on the basis of the session key within only a given period of time (that is, a period of valid time given to the session key). Thus, the given period of time assigned to the session key makes it possible that the authentication can be performed with as few uses use of passwords as possible under the environment with no use of the SSL protocol. Accordingly, even if a communication terminal 2 with a CPU and a memory whose data storage capacity is smaller is used, a data data transfer speed can be avoided from being reduced. Further, unauthorized accesses to the server system 1 can be prevented, so that security for this authentication system is raised remarkably.

Please replace the paragraph beginning on page 19, line 27 with the following amended paragraph:

Still further, in the present embodiment, the communication terminal 5 is composed of any one selected from a group of the navigation terminal 5, PC3, and mobile phone 4. This group may include a personal digital assistant ~~assistance~~. Thus, the communication terminal is higher in versatility in selecting a desired one and use thereof.

Please replace the paragraph beginning on page 19, line 34 with the following amended paragraph:

Referring to Figs. 12 to 14, a second embodiment of the present embodiment will ~~with~~ now be explained. This second embodiment will exemplify registration ~~resignation~~ for assigning a plurality of communication terminals to one access key. Such a practical case is that one person owns a plurality of vehicles on each of which a navigation terminal is mounted and one access key is given in common to the plural vehicles.

Please replace the paragraph beginning on page 20, line 21 with the following amended paragraph:

On reception of the easy sign-up ~~sing-up~~ data, the server system 1 performs authentication through an inquiry whether or not the received user ID has been registered in the server system 1, whether or not both the received user ID and password is valid, and an access key is yet to be issued (steps S104 and S105). When the inquiry shows a negative result (NG), it is further determined at step S106 if or not it is possible to conduct additional registration. In the case that the additional registration is impossible to perform (NO at step S106), the processing is shifted to step S107, wherein an error code is generated, before going to step S108.

Please replace the paragraph beginning on page 20, line 31 with the following amended paragraph:

The above determination whether or not the additional registration is executable is employed to take into it account a limit in the number of vehicles allowed to participate in the additional registration and a situation that a service provider does not allow the additional registration. For instance, in the case that, due to the service provider's setting, the number of vehicles allowed to participate in the additional registration with no additional charge is two, the determination at step S106 becomes negative (NO) for the additional registration of the third vehicle. In this case, the user is obliged to abandon the additional registration or delete (overwriting) one or more navigation terminals 5 that have been registered. How the additional registration is set up depends on the specifications given by a service provider. It is therefore possible to allow three or more vehicles (in the above example) to be registered additionally for an extra charge.

Please replace the paragraph beginning on page 22, line 20 with the following amended paragraph:

Responsively, the second navigation terminal 5 receives searched results of the registered terminals (navigation terminals) and the additional conditions (step S122). As shown in Fig. 13, in the case of the overwriting processing (YES at step S123), the second navigation terminal 5 responds to a user's operation to designate a navigation terminal to be deleted by overwriting a

new one thereon. In contrast, in the case that the overwriting is not ~~intended~~ ~~indented~~ (NO at step S123), a further determination whether or not the additional registration is desired is determined at step S125. When the additional registration is desired (YES at step S125) with the additional conditions acceptable for the user (YES at step S126), an additional processing code is generated (step S127). On the other hand, the additional registration is not desired (NO at step S125) or the additional conditions are not acceptable for the user (NO at step S126), processing for canceling the additional registration is carried out.

Please replace the paragraph beginning on page 25, line 9 with the following amended paragraph:

Then, the navigation terminal 5 transmits, to the ~~server~~ ~~server~~ system 1 via the Internet IN, the user ID, password, and hardware number, together with the manufacturer ID and model number ID given to the navigation terminal 5, as easy-sign-up data (step S153).

Please replace the paragraph beginning on page 26, line 29 with the following amended paragraph:

Referring to Figs. 16 and 17, a fourth embodiment of the authentication system according to the present invention will now be described. In Fig. 16, the components which are the same ~~as~~ ~~or~~ as or similar to those illustrated in Fig. 1 will now be noted by the references which are the same as those in Fig. 1.

Please replace the paragraph beginning on page 27, line 33 with the following amended paragraph:

The common authentication unit 12a is configured to ~~make~~ ~~makes~~ an authentication cache storage installed therein, so that it can be determined if both of a user ID and a session key are valid or not. This makes it possible to authenticate a ~~session~~ ~~ession~~ key generated by the server system 1. Accordingly the unit 12a is in charge of administrating the user ID and session key.

Please replace the paragraph beginning on page 28, line 12 with the following amended paragraph:

The database unit 15a memorizes all kinds of data necessary for navigation processing, including data indicative of a user ID, session key, and expiration time of the session key; map data to be displayed on a display screen of the navigation terminal 5; various kinds of data required for route processing; both positional data and content data at various points on a map to be displayed on the display screen of a navigation terminal 5; point data necessary for execution of navigation processing; and users' data about users who use the navigation terminal 5. These kinds of data are read out at necessary timing from the database 15a and sent to the system controller 13a ~~controller13a~~.

Please replace the Abstract with the amended Abstract on a separate sheet included in the Appendix.